The Report Committee for Kenneth Donaldson Meiser
Certifies that this is the approved version of the following report:

Opening Pandora's Box:
The Social Security Number from 1937-2018

APPROVED BY
SUPERVISING COMMITTEE:

_____

Kathleen Suzanne Barber, Supervisor

_____

Craig Blaha

Opening Pandora's Box:
The Social Security Number from 1937-2018

by

Kenneth Donaldson Meiser

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Identity Management and Security

The University of Texas at Austin

May 2018

Acknowledgements

I want to offer sincere thanks to the faculty of and staff (past and present) of the UT Center for Identity and the UT iSchool for launching the Masters of Science in Identity Management and Security program and supporting the first cohort through five (or six) semesters to graduation. Particular thanks go to Dr. Suzanne Barber, whose vision made the program possible and agreed to supervise this paper. Dr. Craig Blaha generously helped supervise this effort- I hope I produced something worthy of both of your mentorship. I'm grateful for my classmates, I learned so much from each of you and enjoyed every minute we spent together.

Scott Carter, my boss and the CEO of ID Analytics was unwavering in his support. He provided financial support, time away from the office as well as regular encouragement. My IDA teammates put up with a lot and were similarly supportive.

Finally, to my wife, Katie: who supported the crazy idea that her 50-year-old husband who spent way too much time away from home on work trips and already had two kids in college should go back to grad school after a 25-year absence from campus. You've shown me for years what selflessness and true determination look like, and I'm grateful every day for the life we've made.

Opening Pandora's Box:
The Social Security Number from 1937-2018

Kenneth Donaldson Meiser, MSIMS

The University of Texas at Austin, 2018

Supervisor: Kathleen Suzanne Barber

ABSTRACT

Social Security Numbers (SSNs) are an integral part of modern-day American life. The use of the SSN has expanded far beyond the original intent. This expansion has led to significant unintended consequences. This paper examines critical aspects of the Social Security Number: history and construction, expansion of use cases and the unintended consequences thereof, a review of federal studies and reports that outline the ongoing risk and describe efforts to reduce use of SSNs in federal programs.

Additionally, the paper will compare the Social Security Number as a de-facto national identifier to other national identifying schemas and discuss why these other systems do not seem to pose the same risk to personal identity as the Social Security Number.

Finally, the paper discusses a set of guiding principles for future use of the SSN, or if the SSN is replaced; operating principles for whatever future central identity system replaces it, in order to reduce the risk of fraud and misappropriation of identities that impact citizens, enterprises and the government.

Table of Contents

ABSTRACT v

LIST OF TABLES ix

LIST OF FIGURES x

INTRODUCTION 1

THE SOCIAL SECURITY ACT AND REGISTRATION 3

THE SOCIAL SECURITY NUMBER FORMAT 6

Area Numbers 7

Group Numbers 12

Serial Number 13

Construction, Validity and Insight on SSN Issuance Trends 14

Limitations of Construction 17

EXPANDED USE OF THE SSN 19

Expanded Use Cases 19

RISK RECOGNITION 26

Authenticators vs Identifiers 28

Identity Theft and National Security 29

Breaches, Data Brokers and the DarkWeb 32

The Dark Web and Information Sales 34

RISK REDUCTION ACTIVITIES 37

Backing away from the SSN- (costs and effort) 37

DOD and the VA 37

Medicare 39

SSN Randomization 42

Synthetic Identity Fraud 44

ALTERNATE IDENTITY SYSTEMS 48

CONCLUSIONS.....51

APPENDICES.....54

REFERENCES.....60

LIST OF TABLES

Table 1- Assignment by SSA Area Number 10

Table 2- Assigned Ranges By State 11

Table 3- Group Order Assignment 13

Table 4- Final Published High Group Listing- June 2011 16

LIST OF FIGURES

Figure 1- IRS Form 1040 (1962) 21

Figure 2- IRS Form 1040 (1987) 24

Figure 3- ICIT Screenshot of Alpha Bay Listing Dated 1/18/2017 of Equifax and Transunion Credit Reports Available for Sale 35

Figure 4- Sample New Medicare Card (2018) vs Earlier Version (right) 41

Figure 5- ID Analytics: Comparison of the Natural Growth of New SSNs Pre- and Post-Randomization 46

INTRODUCTION

In 1935, as part of the Roosevelt Administration's New Deal, Congress passed and The President signed the Social Security Act. The Act has had many effects on modern American life but arguably, the Social Security Number has the most pervasive day-to-day impact. The Social Security Number (SSN), is a simple 9-digit identifier originally envisioned solely as a way to link a person to their pension and disability benefits account. Use of the Social Security Number has expanded far beyond the original intent and by the late twentieth century, it was the de-facto identifier for almost all citizen interactions with government agencies, financial services companies, employers, schools, and healthcare providers. In many ways, it has become impossible to interact in modern American society without providing your SSN.

Ubiquity has consequences and risks, though. The SSN was 'both public and secret'- public in that it was issued by the government and freely used as an identifier, and secret in that it is presumed to be known only to the legitimate owner and difficult to verify or refute when asserted. It was used as both an identifier and as an authenticator (and as I will discuss later, those two uses are at odds with each other). Because it was created for a limited purpose and before a time when digital communication was commonplace, the format and construction had minimal safeguards now built into modern common numbering schemas. In fact, its predictability made it easy to decipher and counterfeit.

In this paper, I will provide a definitive history of how this basic benefits account number became central to modern American society; how governments, institutions and citizens began to understand the risks associated with expanded use of the SSN and the steps that have recently

been taken to reduce our reliance on it. Additionally, I will examine how other nations implement national identifying schemes without the risks seen in the use of Social Security Numbers. Finally, I will present some potential guidelines for development of a solution to mitigate these risks.

THE SOCIAL SECURITY ACT AND REGISTRATION

As a consequence of the Great Depression in 1929 and the rise of Franklin Roosevelt's New Deal, a significant amount of policy attention began to focus on the idea of creating a pension system for the elderly. According to Dewitt "fewer than 10 percent of American workers had any kind of private pension" (DeWitt, 2010, p3). President Roosevelt directed then Secretary of Labor Frances Perkins to devise a sustainable old-age insurance system (Altmeyer, 1966, p7)

Secretary Perkins and the Department of Labor's Committee on Economic Security created a plan and enabling legislation that was submitted to Congress on January 17, 1935 (Dewitt, 2010, p4). The Social Security Act was signed by President Roosevelt August 14, 1935. The act was not without controversy; funding formulas, the idea of socialized pensions and forced employer payroll deductions as well as the concept of mandatory registration of all working citizens were fiercely debated during the 1936 Presidential and Congressional campaign season. (Altmeyer, 1966, p69)

Shortly before election day, the *New York Journal American* and other Hearst Newspapers published an editorial cartoon and a front-page article attacking the plan. The cartoon shows a masked man, with his shirt removed, suggesting enslavement and wearing a numbered dog tag. (Smith, 2003, p205). The opposition to national registration and the Social Security Act itself was not only from Republicans and conservative quarters, organized labor had concerns that the SSN could be used by employers to suppress union organization by identifying and blacklisting organizers (Parenti, 2003, p85). Many on the left also saw parallels to citizen registration

programs taking place in Fascist Italy, Spain and in Nazi Germany. (Hearing- Use of SSN as a National Identifier, 1991)

Even with a 1937 program go-live date, the newly-established Social Security Board delayed initial registration until November 16, 1936, just under two weeks after the 1936 election was complete and less than 50 days before the program was to go live. Social Security Board Chairman Arthur Altemeyer also directed that the term "Assignment of Social Security Numbers" be used in all official communication in lieu of the politically-charged term "registration" (Altemeyer, 1966, p70) Furthermore, Altemeyer sought assistance from the Postal Service, which at the time was the most-trusted government entity (Smith, 2003, p205) and had the necessary local footprint of over 45,000 post offices (Puckett, 2009, p60) to issue and collect the required forms.

Treasury Decision 4704 was the enabling regulation directing the "assignment" of SSNs and Employer Identification Numbers and was formally published November 6, 1936, just a few days after the election (Title 26, CFR, 401{G}, 1936). The Post Office and Social Security Administration distributed the new SSA form SS-5 *Application for a SSN* to employers in late November, 1936 (Puckett, 2009, p60) with directions to employees to complete and return the forms back to the employer, to their labor organization, or their local post office. (Wyatt and Wandel, 1937, p54). Amazingly, 4 weeks after the first SS-5 forms were distributed to employers; the Post Office reported over 22 million completed applications had been received, which was 85% of the expected initial volume. (Wyatt and Wandel, 1970, p62) By August 31, 1937 the SSA had logged over 33.4 million applications.

The original SS-5 collected only a few fields of data: employee name, address, employer name and address, age, date of birth, place of birth, sex and color (Puckett, 2009, p58). The current form, last revised in 2011, adds additional fields for prior names, citizenship, ethnicity, phone number as well as parental names and SSNs. (SSA Form SS-5, 2011) During the original SSA application period many employers attempted to distribute additional forms requesting information regarding nationality, union affiliation, religion, and educational data. The practice was apparently common enough that in January 1937 the SSA was forced to issue public warning to employers and employees about this unauthorized practice. (Wyatt and Wandel, 1937, p57)

Even before the first SSN was issued, there was clear demonstration of the value and sensitivity associated with data collection and systemic citizen registration that continue to the present day. The Social Security Board needed an enumeration scheme to effectively administer the social welfare programs, but the registration process enabled foes of the Social Security Act to use fear tactics to raise concerns over the entire program. Employers used the enumeration process to gather additional, non-authorized data and regulators were forced to respond with assurances to citizens and sanctions to employers. The pattern of data collection and common indexing schemes foreshadow debates still underway.

THE SOCIAL SECURITY NUMBER FORMAT

With an estimated 405 million SSNs issued, most Americans are likely familiar with the form of a Social Security Number: 3 digits, a dash, two digits, another dash and then four more digits: (123-45-6789). Many citizens are likely unaware that the format was originally created to support regional issuance of numbers and that until recently, the number format indicated both the state associated with the postal address of the applicant and a date range of issuance.

In 1935 and 1936, the newly formed Social Security Board considered many schemas for identifying account holders, one original draft plan suggested an 8-digit alphanumeric with 3 alphabetic characters representing geography and 5 digits to represent the person to whom the card was assigned. (Puckett, 2009, p3) This plan was cancelled almost immediately based on feedback from other government agencies such as the Census Bureau and the Bureau of Labor Statistics (BLS) whose data processing equipment was not capable of processing alphanumerics. (Puckett, 2009, p3) Additionally, the Social Security Board was notified that the two manufacturers of tabulating equipment capable of processing alphanumeric data in 1936 were being sued by the Department of Justice for violations of the Sherman Anti-Trust Act. (Cronin, 1985) The Social Security Administration official history drily notes that this might be "the first inkling that the embryonic agency was given of the tremendous impact machines would have on the way it would do business" (Cronin, 1985)

Bearing in mind these objections and leveraging the expertise of agencies with more experience, the SSA formed an interdepartmental subcommittee with representation from the BLS, Census,

the Labor Board and the Central Statistical Agency. The committee established three alternative schemas for consideration. (Puckett, 2009, p4)

- Eight numeric digits, with a three-digit geographic indicator and a 5-digit serial number
- Seven alphanumerics with three alpha characters and four digits.
- A nine-digit number made up of three parts: A four-digit sequence number, a two-digit birth year indictor and a three-digit geographic identifier.

In February of 1936, the committee agreed to use a variation of the nine-digit option replacing the age component with a year-of-issuance indicator in the two-digit segment. (Puckett, 2009, p7) Later in 1936 a final format change was proposed: the year-of-issuance indicator in the two-digit segment was replaced with a group number that could proxy year of issuance and would allow the SSA to expand the possible SSN combinations to nearly one billion unique identifiers. (McKinley and Frase, 1970, 342-344) This format continues today but the geographic and issuance time indicators were disestablished in the June 2011 SSN randomization changes which will be discussed later in this paper. In this adopted numbering scheme, the format was established using the following rules:

- The first three digits were referred to as the Area Number
- The fourth and fifth digits were designated as the Group Number
- Digits six through nine were labelled as the Serial Number

Given these basic guidelines, further rules and procedures to determine how Area, Group and Serial numbers were assigned to applicants were established by the Social Security Board.

Area Numbers

Ranges of Area numbers were assigned to individual states based on the current population and expected population growth. Each state was assigned to one of 12 regional SSA offices. These locations were:

I.	Boston	VII.	Birmingham
II.	New York	VIII.	Minneapolis
III.	Philadelphia	IX.	Kansas City
IV.	Washington	X.	San Antonio
V.	Cleveland	XI.	Denver
VI.	Chicago	XII.	San Francisco

(SSA Circular No 9, 1936).

SSNs issued before late 1972 were issued by one or more local offices, which were subordinate to the regional office and located the state of issuance. (SSA POMS, 1989)

Area numbers assigned to states were assigned in numerical order, generally running from east to west. Under this method, northeastern states have the lowest Area Numbers and numbers generally increase as assignment moves west and south. The Social Security Administration indicates that Group 001 was assigned to New Hampshire, even though Maine is more easterly and extends to the north of New Hampshire. This is because former New Hampshire Governor John Winant had been named the original director of the Social Security Board and was slated to be the first-recipient of a Social Security Number. The SSA wanted that number to be the lowest possible number (001-01-0001). Governor Winant declined the honor and this number was assigned to another New Hampshire resident (Long, 1993, p83).

Table 1 provides the states assigned to specific Area Numbers as of June 2011 when this geographic assignment was phased out. Table 2 provides a list of assigned area Numbers by State

Table 1- Assignment by SSA Area Number

Assignment by SSA Area Number					
Area Number	**State Assignment**	**Area Number**	**State Assignment**	**Area Number**	**State Assignment**
000	INVALID	429-432	AR	586	GU
001-003	NH	433-439	LA	587-588	MS
004-007	ME	440-448	OK	589-595	FL
008-009	VT	449- 467	TX	596-599	PR
010-034	MA	468-477	MN	600-601	AZ
035-039	RI	478-485	IA	602-626	CA
040-049	CT	486-500	MO	627-645	TX
050-134	NY	501 - 502	ND	646-647	UT
135-158	NJ	503-504	SD	648-649	NM
159-211	PA	505-508	NE	650-653	CO
212-220	MD	509-515	KS	654-658	SC
221-222	DE	516-527	MT	659-665	LA
223-231	VA	518-519	ID	666	INVALID
232	WV* NC	520	WY	667-675	GA
233-236	WV	521-524	CO	676-679	AR
240-246	NC	525	NM	680-690	NV
247-251	SC	526-527	AZ	691-699	VA
252-260	GA	528-529	UT	700-728	RAILROAD
261-267	FL	530	NV	729-733	ENUMERATION AT ENTRY
268-302	OH	531-539	WA	734-749	UNASSIGNED
303-317	IN	540-544	OR	750-751	HI
318-361	IL	545-573	CA	752-755	MS
362-386	MI	574	AK	756-763	TN
387-399	WI	575-576	HI	764-765	AZ
400-407	KY	577-579	DC	766-772	FL
408-415	TN	580 #	USVI/PR	773-899	UNASSIGNED
416-424	AL	581-584	PR	900-999	IRS ITIN ^
425-428	MS	585	NM		

*- Group 30 assigned to NC

^- 70 or 88 in the positions 4 and 5 prior to April 11 2011. After April 11, 2011, 70-88, 90-92 and 94-99 (inclusive)

Source:https://www.irs.gov/individuals/international-taxpayers/general-itin-

Table 2- Assigned Ranges By State

Assigned Ranges By State					
State Assignment	Area Numbers	State Assignment	Area Numbers	State Assignment	Area Numbers
Alaska	574	Massachusetts	010-034	Pennsylvania	159-211
Alabama	416-424	Maryland	212-220	Puerto Rico	580-584, 596-599
Arkansas	429-432, 676-679	Maine	004-007	Rhode Island	035-039
Arizona	526-527, 600-601, 764-765	Michigan	362-386	South Carolina	247-251, 654-658
California	545-573, 602-626	Minnesota	468-477	South Dakota	503-504
Colorado	521-524, 650-653	Missouri	486-500	Tennessee	408-415, 756-763
Connecticut	040-049	Mississippi	425-428, 587-588, 752-755	Texas	449- 467, 627-645
DC	577-579	Montana	516-527	US Virgin Islands	580
Delaware	221-222	North Carolina	232*, 240-246	Utah	528-529, 646-647
Florida	261-267, 589-595, 766-772	North Dakota	501 - 502	Virginia	223-231, 691-699
Georgia	252-260, 667-675	Nebraska	505-508	Vermont	008-009
Guam and Pacific Islands	586	New Hampshire	001-003	Washington	531-539
Hawaii	575-576, 750-751	New Jersey	135-158	Wisconsin	387-399
Iowa	478-485	New Mexico	525, 585, 648-649	West Virginia	232*-236
Idaho	518-519	Nevada	530, 680-690	Wyoming	520
Illinois	318-361	New York	050-134	INVALID	000, 666
Indiana	303-317	Ohio	268-302	Railroad Retirement system	700-728
Kansas	509-515	Oklahoma	440-448	Enumeration at Entry	729-733
Kentucky	400-407	Oregon	540-544	UNASSIGNED	734-749, 773-899
Louisiana	433-439, 659-665			IRS ITIN ^	900-999

*- Group 30 assigned to NC

^- 70 or 88 in the positions 4 and 5 prior to April 11 2011. After April 11, 2011, 70-88, 90-92 and 94-99 (inclusive) Source: https://www.irs.gov/individuals/international-taxpayers/general-itin-information

An examination of these tables indicates the Social Security Administration was required to assign additional Area Number ranges to high growth states. For example; Texas, originally assigned 19 Area Numbers (449-467) which supported 18,808,119 unique SSN assignments (19 x 99 x 9,999) ran out of numbers and was assigned an additional set of 19 Area Numbers (627-645) which began to be used in 1998 (SSA POMS, 1989)

Group Numbers

The fourth and fifth digit of a Social Security represent a block, or group of SSNS issued within a given Area Number. There are 99 available groups within each Area Number because Group 00 is never assigned. (SSA POMS, 1989) Originally designed as a mechanism to facilitate simultaneous but unduplicated issuance by multiple offices within an assigned SSN area, the groups provide insight, but not absolute reference to the time frame in which the given SSN was issued. Regardless of the assigned Area Number, the Group number issuance order follows a common pattern. (SSA POMS, 1989) This pattern is not strictly sequential, it follows the order below:

- First, Odd-Numbered groups from 01 to 09
- Second, Even-numbered groups from 10-98
- Third, Even-numbered groups from 02-08
- Finally, Odd-numbered groups from 11-99

Thus, the prescribed order of Group Number issuance for a given area would be as depicted in Table 3.

Table 3- Group Order Assignment

01	03	05	07	09	10	12	14	16	18	20
22	24	26	28	30	32	34	36	38	40	42
44	46	48	50	52	54	56	58	60	62	64
66	68	70	72	74	76	78	80	82	84	86
88	90	92	94	96	98	02	04	06	08	11
13	15	17	19	21	23	25	27	29	31	33
35	37	39	41	43	45	47	49	51	53	55
57	59	61	63	65	67	69	71	73	75	77
79	81	83	85	87	89	91	93	95	97	99

Because all Group Numbers associated with a given set of Area Numbers were issued before moving to the next Area Number, these combined Area and Group Numbers in the first 5 digits of a Social Security Number can be assigned to a specific region and time. This ability to reverse-engineer a SSN would later create a method for disclosure as SSN use cases expanded. (Acquisti, 2009)

Serial Number

The last four digits of the SSN comprise the Serial Number. This number was assigned sequentially within an Area/Group. The Serial Number 0000 is never assigned, thus for each Area/Group; 9,999 serial numbers are available for assignment. (Puckett, 2009, p58)

Construction, Validity and Insight on SSN Issuance Trends

NOTE: These rules of Constructions and Validity apply ONLY to SSNs issued prior to June 2011 when the Social Security Administration implemented a policy known as SSN Randomization- the reasons behind and impacts of randomization will be discussed later in this paper.

Given the rules above and the supplied tables, one could determine that a Social Security Number beginning with the three-digits of 450 was issued in Texas and that one that began with 001 was issued in New Hampshire Furthermore, we can establish that the SSN 001-07-XXXX was issued many years prior to SSN 001-02-XXXX, even though the Group Number 02 is numerically lower than the 07 Group. Finally, we can tell that SSN 001-07-9900 was issued before SSN 001-07-9950 given the strict sequential order of the Serial Number assignment. With the knowledge of when a given person's SSN was issued, one can determine whether any other SSN issued within the State or Territory associated with a given Area Number was issued before or after the known SSN. Additionally, the Social Security Administration published a monthly "High Group Listing" which provided an indication of the current Group in a given Area from which SSN are being issued. A copy of the Final High Group List, published by the Social Security Administration in June 2011 is depicted in Table 3 below. A Group indicator of

99 associated with an Area number indicates the Area number is completely assigned and these Group Numbers are notated with gray fill in the table cell.

Additional Insights are inferred from this table. Using the example above that discussed the initial (449-467) and secondary ranges (627-645) assigned to SSNs for Texas, we can determine that as of June 2011, somewhere over 30 million SSNs had been issued to Texans- the 18.8 million from the initial Area range described above and at least 12 million from the second range. With 18.8 million numbers available form this second range, an analyst can determine that this range is already almost two-thirds exhausted and could forecast the rate of consumption/exhaustion of available numbers. This exhaustion of numbers within an assigned Area range was one contributing factor the SSN randomization that will be discussed in a later section.

Table 4- Final Published High Group Listing- June 2011

HIGHEST GROUP ISSUED AS OF 06/24/11

This list shows the SSN area and group numbers that are in the process of being issued as of the date at the top of this page.

NOTE: * INDICATES GROUP CHANGE SINCE LAST MONTH.

001 11	002 11	003 08	004 13	005 13*	006 11	007 11	008 94	009 94*	010 94	011 94	012 94
013 94	014 94	015 94	016 94	017 94	018 94	019 94	020 94	021 94*	022 92	023 92	024 92
025 92	026 92	027 92	028 92	029 92	030 92	031 92	032 92	033 92	034 92	035 74	036 74
037 74	038 74	039 74	040 15	041 15	042 15	043 15	044 15	045 15	046 15	047 15	048 15
049 15*	050 02	051 02	052 02	053 02	054 02	055 02	056 02	057 02	058 02	059 02	060 02
061 02	062 02	063 02	064 02	065 02	066 02	067 02	068 02	069 02	070 02	071 02	072 02
073 02	074 02	075 02	076 02	077 02	078 02	079 02	080 02	081 02	082 02	083 02	084 02
085 02	086 02	087 02	088 02	089 02	090 02	091 02	092 02	093 02	094 02	095 02	096 02
097 02	098 02	099 02	100 02	101 02	102 02	103 02*	104 02*	105 02*	106 98	107 98	108 98
109 98	110 98	111 98	112 98	113 98	114 98	115 98	116 98	117 98	118 98	119 98	120 98
121 98	122 98	123 98	124 98	125 98	126 98	127 98	128 98	129 98	130 98	131 98	132 98
133 98	134 98	135 25	136 25	137 25	138 25*	139 23	140 23	141 23	142 23	143 23	144 23
145 23	146 23	147 23	148 23	149 23	150 23	151 23	152 23	153 23	154 23	155 23	156 23
157 23	158 23	159 86	160 86	161 86	162 86	163 86	164 86	165 86	166 86	167 86	168 86
169 86	170 86	171 86	172 86	173 86	174 86	175 86	176 86	177 86	178 86	179 86	180 86
181 86	182 86	183 86	184 86	185 86	186 86	187 86	188 86	189 86	190 86	191 86	192 86
193 86	194 86	195 86*	196 84	197 84	198 84	199 84	200 84	201 84	202 84	203 84	204 84
205 84	206 84	207 84	208 84	209 84	210 84	211 84	212 91	213 91	214 91	215 91*	216 89
217 89	218 89	219 89	220 89	221 13	222 11	223 99	224 99	225 99	226 99	227 99	228 99
229 99	230 99	231 99	232 57	233 57	234 57	235 57*	236 55	237 99	238 99	239 99	240 99
241 99	242 99	243 99	244 99	245 99	246 99	247 99	248 99	249 99	250 99	251 99	252 99
253 99	254 99	255 99	256 99	257 99	258 99	259 99	260 99	261 99	262 99	263 99	264 99
265 99	266 99	267 99	268 17	269 17	270 17	271 17	272 17	273 17	274 17	275 17	276 17
277 17	278 17*	279 15	280 15	281 15	282 15	283 15	284 15	285 15	286 15	287 15	288 15
289 15	290 15	291 15	292 15	293 15	294 15	295 15	296 15	297 15	298 15	299 15	300 15
301 15	302 15	303 37	304 37	305 37	306 37	307 37	308 37	309 37	310 37	311 35	312 35
313 35	314 35	315 35	316 35	317 35	318 11	319 11	320 11	321 11	322 11	323 11	324 11
325 11	326 11	327 11	328 11	329 11	330 11	331 11	332 11	333 11	334 11	335 11	336 11
337 11	338 11	339 11	340 11	341 11	342 11	343 11	344 11	345 11*	346 08	347 08	348 08
349 08	350 08	351 08	352 08	353 08	354 08	355 08	356 08	357 08	358 08	359 08	360 08
361 08	362 39	363 39	364 39	365 39	366 39	367 39	368 39	369 39*	370 37	371 37	372 37
373 37	374 37	375 37	376 37	377 37	378 37	379 37	380 37	381 37	382 37	383 37	384 37
385 37	386 37	387 33	388 33	389 33	390 33	391 33	392 33	393 33	394 33	395 33	396 33
397 33	398 31	399 31	400 73	401 73	402 73	403 73	404 73	405 73	406 73	407 73	408 99
409 99	410 99	411 99	412 99	413 99	414 99	415 99	416 67	417 67	418 67	419 67	420 67
421 67	422 67	423 67	424 65	425 99	426 99	427 99	428 99	429 99	430 99	431 99	432 99
433 99	434 99	435 99	436 99	437 99	438 99	439 99	440 29	441 29	442 29*	443 27	444 27
445 27	446 27	447 27	448 27	449 99	450 99	451 99	452 99	453 99	454 99	455 99	456 99
457 99	458 99	459 99	460 99	461 99	462 99	463 99	464 99	465 99	466 99	467 99	468 57
469 57	470 57	471 57	472 57*	473 55	474 55	475 55	476 55	477 55	478 43*	479 41	480 41
481 41	482 41	483 41	484 41	485 41	486 29	487 29	488 29	489 29	490 29	491 29	492 29
493 29	494 29	495 29	496 29	497 29	498 29	499 29	500 29*	501 37	502 37	503 45	504 45
505 59	506 57	507 57	508 57	509 33	510 33	511 33	512 33*	513 31	514 31	515 31	516 49
517 49	518 89	519 87	520 61	521 99	522 99	523 99	524 99	525 99	526 99	527 99	528 99
529 99	530 99	531 71	532 71	533 71	534 71	535 71	536 71	537 71	538 71	539 71*	540 83
541 83*	542 81	543 81	544 81	545 99	546 99	547 99	548 99	549 99	550 99	551 99	552 99
553 99	554 99	555 99	556 99	557 99	558 99	559 99	560 99	561 99	562 99	563 99	564 99
565 99	566 99	567 99	568 99	569 99	570 99	571 99	572 99	573 99	574 61	575 99	576 99
577 53	578 53	579 53	580 41*	581 99	582 99	583 99	584 99	585 99	586 67	587 99	588 09
589 99	590 99	591 99	592 99	593 99	594 99	595 99	596 94*	597 92	598 92	599 92	600 99
601 99	602 87	603 87	604 87	605 87	606 87	607 87	608 87	609 87	610 87	611 87	612 87
613 87	614 87	615 87*	616 87*	617 87*	618 87*	619 87*	620 85	621 85	622 85	623 85	624 85
625 85	626 85	627 31	628 31	629 31	630 31	631 31	632 31	633 31	634 31*	635 31*	636 31*
637 29	638 29	639 29	640 29	641 29	642 29	643 29	644 29	645 29	646 23	647 21	648 58
649 56	650 62	651 62	652 62	653 60	654 38	655 36	656 36	657 36	658 36	659 24	660 24*
661 22	662 22	663 22	664 22	665 22	667 48	668 48	669 48	670 48	671 48	672 48	673 48
674 48	675 48*	676 22	677 22	678 22*	679 20	680 31	681 24	682 24	683 24	684 24	685 24
686 24	687 24	688 24	689 24*	690 22	691 18	692 18*	693 16	694 16	695 16	696 16	697 16
698 16	699 16	700 18	701 18	702 18	703 18	704 18	705 18	706 18	707 18	708 18	709 18
710 18	711 18	712 18	713 18	714 18	715 18	716 18	717 18	718 18	719 18	720 18	721 18
722 18	723 18	724 28	725 18	726 18	727 10	728 14	729 28	730 28	731 28	732 28*	733 26
750 20	751 18	752 09	753 07	754 07	755 07	756 12	757 12	758 12	759 12	760 12	761 12
762 12	763 12	764 29*	765 27	766 04*	767 02	768 02	769 02	770 02	771 02	772 02*	

Additionally, based on the common or closely aligned Group Numbers within a given range of Area Numbers assigned to a state, one can infer that the Social Security Administration was issuing SSNs from multiple Area Numbers at the same time. Referring back to the New Hampshire Areas discussed earlier: Areas 001 and 002 were issuing from Group 11 and Area 003 was issuing from Group 008 at the time of the final High Group distribution in June 2011. According to the Group issuance order above, 08 and 11 are sequential for issuance and indicate that roughly 55% of the allocated Area/Group combinations for NH had been used as of the June 2011 published date. The second range of Texas Area/Groups exhibits the same pattern.

Furthermore, comparing changes across the monthly SSA High Group Reports provides insight into the issuance rate of SSNs within a given state or territory. Since there are 9,999 SSNs issued for each Area/Group combination; each change on a given High Group List can be cross referenced with earlier High Group Lists to determine an issuance rate.

LIMITATIONS OF CONSTRUCTION

SSN construction rules didn't allow inclusion of any but the most basic verification features to help prove number validity and no mechanism to authenticate its relationship to a person, based on characteristics within the number itself. A 2004 FTC report suggested that the addition of a checksum or even a single check digit, which uses an

algorithm to calculate an additional digit based on the other values in the string, could help eliminate data entry errors or highlight invalid consumer-supplied Social Security Numbers (FTC, 2004, p39).

EXPANDED USE OF THE SSN

Because of the concern expressed about citizen registration and fear about the assignment of a National ID number in the 1936 election cycle, the SSA went to great lengths to assure citizens that the SSN was going to be used exclusively used to manage a person's pension and benefits administered under the Social Security Act. (McKinley and Frase 1970, 357-358) As another method to reassure applicants, Social Security Cards issued from 1946 until 1972 displayed the words "NOT FOR IDENTIFICATION" across the card (Swendiman and Lanza, 2014, p2).

Ironically, it took the SSA less than 1 year to break the understood, but not explicit commitment to not share the SSN with other agencies. (Smith, 2013, p4). The first expansion provided Social Security Numbers to state unemployment and pension boards to coordinate benefit delivery. Arguably, this first expansion supported actions funded by the Social Security Act and the use was not beyond the stated original purpose provided to applicants/account holders.

Expanded Use Cases

Expansion of Social Security Number use inside other agencies of the government began in earnest with Executive Order 9397 *Numbering Systems for Federal Accounts*

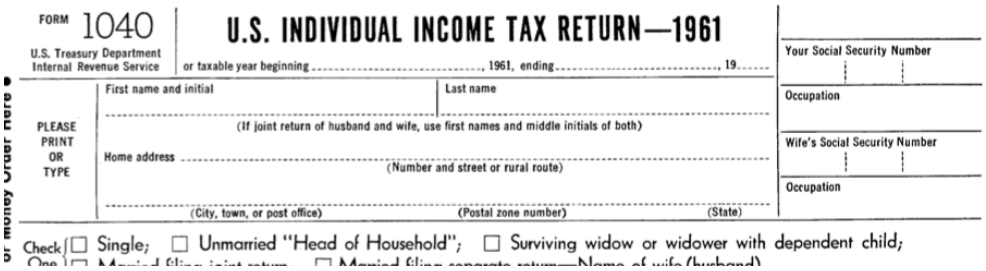
Relating to Individual Persons which was published November 22, 1943. (EO 9397, 1943) The Executive Order acknowledged that Federal agencies needed a common way to identify persons and that 70 million SSNs had already been issued- many to members of the Federal workforce. Because of this already-in-place capability, the order established that agencies should use SSNs when they 'establish new systems of permanent account numbers pertaining to individual persons". It further directed that the "Social Security Board shall provide for the assignment of an account number who is required by any Federal agency to have such a number" and provided for reimbursement to the Social Security Board for the creation of these systems. (EO 9397, 1943)

By the early 1960's increasing computerization of records was driving the need for common reference systems across government agencies and within the private sector.

In 1961, the US Civil Service Commission formally adopted the SSN as the singular identification number for applicants and civil service employees. (Swendiman and Lanza 2014, p2) Incorporation of the SSN was significant because at the time the Civil Service Retirement Program was independent of the SSA and federal employees were not eligible for Social Security benefits.

The 1961 tax filing season (taxes filed for April 15, 1962) was the first year in which the IRS required submission of the filer's Social Security Number. (IRS Form 1040 Filing Instructions, 1961)

Figure 1- IRS Form 1040 (1962)



FORM 1040

U.S. Treasury Department
Internal Revenue Service

U.S. INDIVIDUAL INCOME TAX RETURN—1961

or taxable year beginning ....., 1961, ending ....., 19.....

Your Social Security Number

First name and initial | Last name

Occupation

PLEASE PRINT OR TYPE

(If joint return of husband and wife, use first names and middle initials of both)

Wife's Social Security Number

Home address .....
(Number and street or rural route)

Occupation

(City, town, or post office) (Postal zone number) (State)

Check One ☐ Single; ☐ Unmarried "Head of Household"; ☐ Surviving widow or widower with dependent child;

The 1965 Medicare Act (Public Law 89-384) expanded the 1937 Social Security Act to implement healthcare insurance for the aged. As an expansion of the Social Security system Social Security Administrators determined that a Medicare policy holders system identifier and their identity cards would use the Social Security Number. (Long, 1993, p84)

In 1966 the Veterans Administration adopted the SSN as a primary identifier for the provision of healthcare. (Long, 1993, p84) The use of this identifier is likely a consequence of continued SSN proliferation in other government programs as well as the need to match benefits and allocate costs across the Veterans Administration and Medicare systems. (SSN as National Identifier Hearing, 1991, p63)

The Department of Defense began to transition away from military Serial Numbers in 1969. New recruits in the Army and Air Force began using SSN as their military Serial

number on July 1, 1969. The Navy and Marine Corps converted to SSN use January 1, 1972 and the Coast Guard in October of 1974. (National Archives)

The Bank Secrecy Act of 1970 implemented new record-keeping and reporting requirements for Financial Institutions:

> "Banks are further required to retain records of the taxpayer identification numbers of persons maintaining accounts; in the case of an account of one or more individuals, a bank must maintain a record of the social security number of an individual having a financial interest in that account." (BSA 103.34(b) 1970)

Christian Parenti's *Soft Cage: Surveillance in America from Slavery to the War on Terror* describes increasing demand by the private sector in the 60's for creation of a common national identifier. (Parenti, 2003, p11). The Harvard Business review similarly advocated "*universal adoption of the Social Security number and an address code as identification devices*" in 1961. (Anthony and Sears, 1961, pp 65-71)

Given the IRS requirement for Banks to collect SSNs and link to accounts, it's not surprising that the SSN became the de-facto customer identifier in the Financial Services industry. Retail credit bureaus began the transition to computerized reporting in the late 1960's. Retail Credit Company, later known as Equifax; announced a project to transition to all computerized records (Trainor, 2015) and noted privacy advocate Alan Westin of Columbia University wrote a New York Times Editorial in 1968 stating "transferring information from a manual file onto a computer triggers a threat to civil liberties, to privacy, to a man's very humanity because access is so simple." (Trainor, 2015). These concerns influenced later Congressional hearings and the creation of the Fair Credit

Reporting Act in 1972.

Collection of SSNs in the commercial sector was both a matter of convenience and of regulatory requirement. Appendix 1 provides detail of 11 Federal Statutes governing financial industry collection, verification and disclosure of SSNs to third parties (Financial Services Roundtable, 2018).

With little awareness of the potential implications regarding the dangers of SSN disclosure on the part of the paper or the NYPD, the New York Times published an article in June of 1972 headlined "Police Urge Social Security Numbers on Valuables". The NYPD's Operation Identification encouraged citizens to borrow electric engravers from local precincts and mark "televisions, bikes, silverware and jewelry" to enable recovery of stolen items. (Blumenthal, 1972) in the light of our current level of concern for protecting the SSN, this appears to be terrible advice, but large-scale ID theft was 15-20 years away.

The 1976 Tax Reform Act (Public Law 94-455, 1976) expanded the use of the Social Security Number outside of Federal Agencies by amending the Social Security Act to authorize and direct the use of the SSN in state and local government programs.

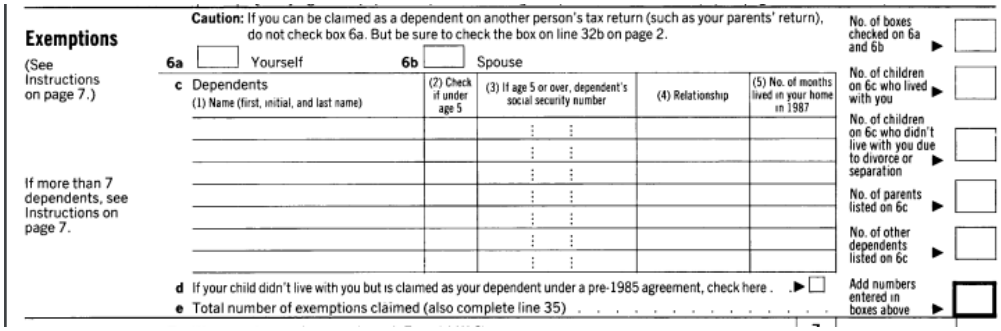
> "It is the policy of the United States that any State (or political subdivision thereof) may, in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction, utilize the social security account numbers issued by the Secretary for the purpose of establishing the identification of individuals affected by such law, and may require any individual

who is or appears to be so affected to furnish to such State (or political subdivision thereof) or any agency thereof having administrative responsibility for the law involved, the social security account number (or numbers, if he has more than one such number) issued to him by the Secretary". (PL 94-455, Sec. 1211(C) (i), 1976)

1982's Public Law 97-365 (the Debt Collection Act) implemented a requirement for collection of a Social Security Number as part of the application process for any Federal Loan program; such as student loans, agricultural loans, Small Business Administration loans and Federal Housing Loans among others. (PL 97-365 Sec 4. (a), 1982)

In 1987 the IRS amended IRS Form 1040 to require the inclusion of SSNs for every dependent aged 5 or more. (PL 99-514 Sec. 1524, 1986) Figure 2 provides a sample of the changed portion of the form.

Figure 2- IRS Form 1040 (1987)



Exemptions (See Instructions on page 7.)

Caution: If you can be claimed as a dependent on another person's tax return (such as your parents' return), do not check box 6a. But be sure to check the box on line 32b on page 2.

6a ☐ Yourself 6b ☐ Spouse

c Dependents

(1) Name (first, initial, and last name)	(2) Check if under age 5	(3) If age 5 or over, dependent's social security number	(4) Relationship	(5) No. of months lived in your home in 1987

If more than 7 dependents, see Instructions on page 7.

No. of boxes checked on 6a and 6b ▶

No. of children on 6c who lived with you ▶

No. of children on 6c who didn't live with you due to divorce or separation ▶

No. of parents listed on 6c ▶

No. of other dependents listed on 6c ▶

d If your child didn't live with you but is claimed as your dependent under a pre-1985 agreement, check here . ▶☐

e Total number of exemptions claimed (also complete line 35) . . . . . Add numbers entered in boxes above ▶

As an example of the challenges in balancing the risks of widespread proliferation of the SSN versus the ability of the SSN to assist in detecting fraud, a 1989 newspaper article pointed out that 7 million fewer children were claimed as dependents that year than in 1986. Given the $1,900 per dependent tax deduction, the elimination of the 7 million seemingly-bogus dependents had a $2.8 Billion positive impact to the US Treasury in just

the 1987 tax year. (LA Times, 1989) The IRS expanded the requirement to provide a SSN for all dependents claimed on tax forms from 1989 on.

Prior to the IRS changes requiring a SSN for dependents, there was little incentive to obtain a SSN for a child and many parents waited until their child needed a SSN, usually coinciding with first employment. In 1988, the Social Security Administration began a program knows as Enumeration at Birth (EAB). This program enables and encourages parents to complete applications for SSNs for newborn babies as part of the state-mandated vital records process SSA statistics indicate that around 96% of SSNs issued to infants are the result of an EAB application. The EAB plan was rolled out nationwide and establishes common processes and technology interfaces and cross-references between the individual State Bureau of Vital Statistics and the Social Security Administration (SSA POMS, 2014)

These expanded use cases had increased the universe of both who needed a SSN and the number of entities who had access to it. Issuance had expanded from wage-earners who needed the SSN to report earnings for pension calculations to non-working dependents and children. The SSN was no longer a benefits number used only by the Social Security Board; it had morphed into a multi-agency identifier that enabled reporting and coordination. Further requirements for private entities to collect the SSN had enabled similar uses in commercial transactions.

RISK RECOGNITION

By the late 1980's the SSN was essential to a citizen's interactions with all levels of government and with many sectors of the private economy, most notably in the areas of banking, finance and consumer credit. The expansion of use cases created an environment where the SSN was:

1. Proliferated across multiple systems in government and commercial enterprises.
2. Commonly disclosed in day to day interactions. Following the 1976 Tax Reform Act, many states added SSN to Driver's Licenses and in jurisdictions like Texas, the SSN was used as the Driver's License number. It was common practice to preprint SSNs on checks to prevent having the clerk copy the information on the back of the check. (Indiana DFI)
3. Often used as a mechanism to prove or authenticate an identity. Prior to the 1990's the extension of credit in the form of auto loans, mortgages or credit cards was generally an extension of an already-in-place banking relationship. As the financial services industry embraced the use of target marketing in the 90's, monoline financial services firms like Capitol One and MBNA experienced explosive growth through the use of sophisticated, data driven marketing campaigns directly to consumers with whom the bank had no prior relationship. (Wheatley, 2014) As an example, Capital One grew credit card lending balances from $5B in 1995 to over $80B in 2014. (Perez, 2015)

4. Computerized underwriting; including the automated ordering of credit scores enabled the extension of credit with no face-to-face verification or identity proofing via physical documents (FFIEC, 2014) The assertion of a Social Security Number in these transactions provided implicit proof that the applicant was the legitimate owner of the identity.

In 2006 the Federal Trade Commission authorized an *Identity Theft Survey Report*. The study involved telephone interviews of a random sample of 4,917 US adults. (FTC 2006). The survey determined that 3.7% of respondents had discovered that they had been a victim of Identity theft in 2005. Extrapolated to the US population, this suggests that 8.3 million adults were affected in 2005, alone.

Further classifying types of identity fraud provides even more insight on the rate of new account fraud, the most common type of fraud associated with SSN compromise. (FTC, 2006) 17% of victims indicated their personal information was used to open at least one new account. The two most common account types opened by fraudsters were telephone accounts (landline and wireless) and credit card accounts. Median loss was $1,350 per person for new account fraud and the average victim reported 10 hours in time spent resolving issues associated with the fraud. (FTC, 2006, p5)

A 2007 Congressional hearing- *Protecting the Privacy of the Social Security Number From Identity Theft* heard testimony from over a dozen witnesses. Testimony from

Daniel Bertoni of the Government Accountability Office summarized the proliferation of and reliance on SSNs:

> "In the private sector, information re-sellers, credit bureau reporting agencies and health care organizations collect SSNs from various sources and use this information primarily for identification verification purposes. Large information re-sellers obtain SSNs from various public records, such as bankruptcy notices, tax liens, civil judgments and property transactions. In addition to their own direct use of SSNs, entities such as banks, securities firms, tele- communications firms and tax preparers also share this information—SSN information with third party contractors who perform services for them." (Protecting the Privacy, 2007)

Authenticators vs Identifiers

Awareness that the use of the Social Security Number as an authenticator was potentially problematic was increasing. In the same 2007 Congressional hearing referenced above, the House Ways and Means Subcommittee on Social Security heard testimony from Annie Anton of North Carolina State University who was speaking on behalf of the Association for Computing Machinery

> "…many businesses use the Social Security number as both an identifier and an authenticator. The terms ''identifier'' and ''authenticator'' have specific technical meanings that are often confused. An ''identifier'' is a label associated with a person. An ''authenticator'' provides the basis to believe that somebody is accurately labeled by some given identifier. So, authenticators might be something you know, like a secret password or a pin, something you have, like the key to your house, and something you are, such as a biometric. A Social Security number is an identifier. It is something that anyone can know, and many

> will, so it is not a secret. Hence, it is unusable as an authenticator." (Anton-Hearing transcript)

Similar conclusions were made in the 2007 FTC Report on SSNs and ID Theft;

> "... SSNs do not function well as authenticators because they are used commonly as identifiers and thus are widely available." (FTC, 2007)

The FTC task force was established by President George W Bush in 2006 and was chartered to develop a national strategy to combat identity theft and fraud. With representatives from the Department of Justice, the Federal Trade Commission and 17 other agencies, the task force recommended changes in government processes regarding SSNs to reduce use of the SSN within agencies, and to develop more robust data breach plans. The task force also examined authentication alternatives but made no specific recommendations other than to continue studying the issue. Finally, the task force recommended standardized reporting procedures and data tracking within law enforcement to improve measurement of and response to ID theft cases.

Identity Theft and National Security

Concern over the compromise of Social Security numbers was not limited to economic crimes. Following the events of 9/11, one thread of investigation related to the methods used by the 19 hijackers to create identities and to hide in plain sight. In 2003, the Senate Finance Committee held a hearing entitled "The Alias Among Us" that examined these issues. (*The Alias*, 2003)

One witness at this hearing was Yousseff Hmimssa, who had pleaded guilty and became a cooperating witness in a criminal trial. Mr. Hmimssa described the process he used to obtain legitimate documents using fraudulent methods

> "I was living in Europe, so I bought a French passport and I came to the United States as a French citizen. So, I got here and went to Chicago in 1994 and I was, at that time, here legally. Then I went and I applied for a Social Security card. I got it in the mail. I went and I applied for a driver's license and ID"
>
> Further elaborating, he indicated "Once I got to the country, I went to the Social Security Administration and I applied for a Social Security card. I applied for it. Within 10 days, I got it in the mail. Using that card, along with the passport, I went to the Secretary of State in Illinois and I got ID and a driver's license."

Hmimssa indicated that the Social Security Administration performed no verification, that the identity on the passport, Patrick Vuillame was fake, as was the document itself. Using the legitimate SSN issued to the Vuillame identity, Hmimssa obtained an Illinois Driver's License, including authority to drive a cab. Hmimssa later took classes and opened a bank account as Vuillame. (*The Alias*, 2003, pp17-23)

Because the Vuillame passport was fake and he wanted to visit family in Morocco, Hmimssa testified he later obtained a fake US birth certificate under then name Edgardo Colon. Using this new Colon identity, he applied for and received a new SSN which he used to obtain another Illinois DL. Finally, Hmimssa used the Colon birth certificate,

Social Security Card and DL to apply for a US passport. (*The Alias*, 2003, pp17-23). This passport was issued and foreign trips were made on the Edgardo Colon identity.

Hmimssa became a cooperating witness after he was asked by members of a Detroit Terror cell to obtain and create additional false identities. (*The Alias*, 2003, pp24-25) Senator Bunning and Chairman Grassley expressed dismay that the SSA had not implemented any significant safeguards to verify submitted documents. (*The Alias*, 2003, p23)

In 2003, the General Accounting Office (GAO) released a report detailing potential deficiencies in the Social Security Administration procedures to verify applicants from immigrants and resident aliens. The GAO indicated that the SSA had partnered with the Department of Homeland Security to verify applicants using DHS's Systematic Alien Verification for Entitlements (SAVE) software. GAO noted deficiencies in collateral verification procedures, notably failures to perform adequate physical verification of documents to check for watermarks and other security features. (GAO-04-12, 2003).

This GAO report indicated that in 2002 SSA issued 5.57 million Social Security Numbers; 4.23 million to citizens and 1.34 million to immigrants. (GAO-04-12, 2003, p9) Cases like those described by Hmimssa likely represent a very small percentage of SSN issuance events, but the risk associated is significant due to the lack of due diligence on the applications.

Breaches, Data Brokers and the DarkWeb

As identity information, including SSNs, became more valuable and more concentrated, the number of large repositories of identity data increased. These repositories became targets for compromise and exploitation, particularly those that linked personal data with a Social Security Number. Society was a long way from the issuance of a paper card with an SSN and microfiche files stored in a government warehouse. Identity had value, and because there was value, there was money to be made protecting and exploiting it.

Proof of this value and the growth of data compromise incidents can be found in many sources. The Gemalto Breach index (breachlevelindex.com) has tracked breaches since 2013 and provides a running tally of events, records compromised and classifications of compromised data. As of March 23, 2018, the total number of records lost or stolen on the Gemalto index was over 9.7 billion records. A summary report on the first half of 2017, which predates notice of the high-profile Equifax breach, indicated Identity theft accounted for 74% of all reported incidents and a record 1.6 billion records were compromised in the first half of 2017. (Gemalto 2017, p 6)

The 149 million record Equifax data breach, announced in September 2017 (J Scott, 2017) brought additional attention on data brokers. These large repositories of identity data are used for a variety of services including risk services, marketing, underwriting and customer management. (FTC, 2014) The track record regarding data security and

breach for data brokers was problematic- Equifax competitor Experian had a series of breaches including a 15 million record breach in 2015, TransUnion had incidents in 2016 and 2013. (Bisson, 2017).

The first major breach of a data broker took place at ChoicePoint in 2005, when fraudsters gained access to 163,000 consumer records (FTC, 2009) by setting up fraudulent accounts.

In a series of breaches between 2005 and 2018, significant information, including Social Security Numbers, Dates of Birth and address history on consumers were compromised. (J Scott, 2017)

In 2014, the FTC published a report on Data Brokers and concluded; "Big Data is big business" the report further discusses that consumers are often unaware of the companies that house data on them, and their practices. (FTC, 2014, p1) The FTC report acknowledges that data brokers provide important benefits and services but cautioned that indefinite storage of data on consumers creates security risks. (FTC, 2014, p48) Having experienced a series of breaches over the past 10 years, these organizations have failed to mount adequate security given the richness of the data they house and the threat they remain under. In a 2017 report, the Institute for Critical Infrastructure Technology argues "Significant technical and non-technical cybersecurity and cyber-hygiene reform

is necessary to protect consumers from the lackadaisical practices of under-regulated data brokers." (J Scott, 2017, p6)

THE DARK WEB AND INFORMATION SALES

Almost anyone who has picked up a newspaper or seen a movie in the past 15 years has heard the term Dark Web but other than a vague image of an internet back-alley with shadowy figures selling stolen goods, stolen data, drugs and other illicit goods, most people would likely be at a loss to explain exactly what the dark web is and how it works. In short, the darkweb is an assortment of tens or hundreds of thousands of websites that use services designed to hide their IP addresses, physical location and ownership. (Greenberg 2014)

There are a variety of sites on the dark web that exist for legitimate reasons- the most famous example is WikiLeaks, which seeks to support whistleblowers and disclose information that powerful interests want to remain secret. With that said, when many people think of the internet they likely think of sites like the Silk Road where drugs were sold or FBI raids on sites trading in child pornography. Another type of illicit trafficking is taking place on the dark web, and that is the trade in stolen identities. Some Dark Web marketplaces like AlphaBay packages of bundled identities containing Names, address, phone, Social Security Numbers and dates of birth for prices as low as $.25 per record. (Glick, 2016)

The Institute for Critical Infrastructure Technology (ICIT) posted screenshots of credit profiles offered for sale on AlphaBay, a dark web site. These listing promised Personal Information, Scores and tradeline data in their September 2017 report on the Equifax breach (J Scott, 2017, p7)

Figure 3- ICIT Screenshot of Alpha Bay Listing Dated 1/18/2017 of Equifax and Transunion Credit Reports Available for Sale

A perfect storm had formed. America had adopted the SSN as a default identifier but had confused identification with authentication. Government and Commercial entities had linked identities and performance data to a single reference number. Structural weaknesses in how the SSN was calculated created opportunities for impersonation and reverse-engineering. Gaps in the process to issue Social Security Numbers allowed criminals and people who posed national security risks to obtain legitimate SSNs.

Because the SSN was now a proxy for a person and their behavioral attributes, this lack of security and verification could be exploited by bad actors. Demand for this exploitable information created a marketplace for compromised identities and drove large-scale data breaches.

RISK REDUCTION ACTIVITIES

Backing away from the SSN- (costs and effort)

The government had embedded the SSN in a multitude of government and private-sector systems and created laws and regulations mandating the collection, storage and distribution of data on citizens using their Social Security Numbers. However, after 2007, plans and discussions within the government began in earnest to reduce proliferation of Social Security Numbers.

As a response to the President's SSN task force, a number of congressional hearings and the growing understanding that SSN misuse was a major challenge for government, the private sector and citizens, President Bush revised Executive Order 9397. This change directed that agencies "should conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use." (Swendiman and Lanza, 2014, p4)

DOD AND THE VA

The Veterans Administration and the Military started the process to remove SSNs from identification cards and from ID systems, except those responsible for payroll tax reporting and security. Beginning June 1, 2011, replacement ID cards with unique DOD identification numbers were issued in place of military identification containing the SSN (Swendiman and Lanza, 2014, p5)

The removal program was planned to be completed in 3 phases: Phase One removed SSNs from Dependent ID cards began in 2008 and was completed in December of 2012. Phase Two, which began in 2011; removed visible SSNs from DOD Common Access Cards (CAC) Identification Cards. Phase Three is a longer process to remove embedded SSNs from barcodes on CAC cards and USID for civilians. This process is expected to extend until 2022. (DOD CAC 2014) A KUOW news reports suggests the phase Two removal of SSNs from display on ID cards was complete in 2015, but reinforced the 2022 deadline for removal of the Social Security Numbers embedded in the barcodes on IDs (KUOW, 2015)

A 2007 Cost-Benefit analysis conducted by students of the Naval Postgraduate School (Opria and Maraska, 2007) to determine the economics of removal and substitution of the SSN across DOD and Veteran programs. They reported that the Congressional Budget Office had calculated a $50 million five-year cost associated with HR 5835, the Veterans Identity and Credit Security Act of 2006, but the estimated cost of a breach similar to the 17 million record VA breach of 2005 could approach $1 Billion. (Opria and Maraska, 2007 p10-11)

Opria and Maraska also attempted to develop cost models for transition away from the SSN to a Military Identification Number (MIN). One approach approximated cost based on Y2K conversion budgets where millions of lines of code had to reviewed and remediated to change data formats to handle the date transition associated with the year

2000. Based on an estimate of Department of Defense (DOD) and Veterans Administration (VA) systems containing identity data versus those that used date fields as part of the operations, a ratio of 10%- 25% of affected systems was used to estimate costs. (Opria and Maraska, 2017, p 61) Using DOD and VA Y2K remediation costs, Opria and Maraska estimated the cost to remove, replace and test a Military ID Number at somewhere between $73-$174 million. Using a series of other methodologies, the authors estimated a range of between $73 and $200 million to remediate DOD and VA systems. Annual cost reduction/avoidance figures from the change were estimated between $222 to $881 million. (Opria and Maraska 2017, p 61)

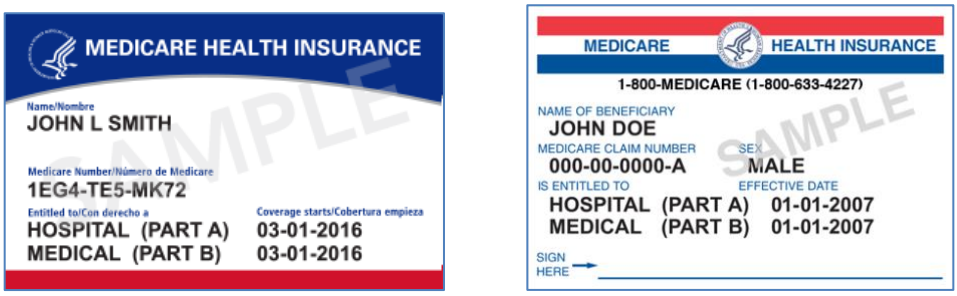
MEDICARE

The Office of the Inspector General of the Social Security Administration produced a report in 2006 that identified risks and system vulnerabilities associated with the display of SSNs on medical documents and ID cards and suggested a set of additional controls. (SSA OIG, 2008, p4) SSA management agreed with these recommendations and agreed to work to reduce this exposure. 2 years later, the OIG issued a follow-on report reviewing progress and found that little to no progress had been made and that estimates for completing a project to replace the SSN on Medicare cards was in the range of five to ten years and over $300million in expected costs. (SSA OIG, 2008, p5) Furthermore, the OIG report noted the plan remained unfunded and no estimate of actual completion was forecast by SSA management.

The House Ways and Means Committee held a hearing in August concerning feasible options for HHS and CMS to remove SSNs from Medicare cards. CMS representatives testified that cost estimates now approached $845 million to remove SSNs from Medicare cards. (House Subcommittee on Social Security, 2012) Suggestions for alternate approaches included truncation of the SSN or replacement with a "Medicare Beneficiary Identifier." (GAO-12-949T, 2012) Unsatisfied with this response from the SSA and the Centers for Medicare and Medicaid Services, the House passed the Medicare Identity Theft Prevention Act of 2012 (HR 1509, 2012), directing the Secretary of Health and Human Services to remove SSNs from Medicare cards. HR 1509 did not become law as no vote on the measure was taken by the Senate.

Ultimately, it was not until the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA)was passed that a deadline was set for elimination of the SSN from Medicare identification cards. MACRA required this change be completed by April 2019. The Centers for Medicare and Medicaid Services has announced that this process is on schedule for April 2018. (CMS, 2018)

Figure 4- Sample New Medicare Card (2018) vs Earlier Version (right)



In October 2017, Privacy Journal reported that the IRS was considering changes to IRS Regulations that would allow for truncation of the last 4 digits of a Social Security number on W-2s and 1099 tax and income reporting documents. This change was in response to Congressional guidance issued in September of 2016. The report noted that "limiting identity to the last four digits provides only 'partial protection'". (Privacy Journal, 2017)

These government efforts were remarkable in that they represented the first attempts to reduce reliance on the SSN and to control dissemination. Removing SSNs from Military IDs and Medicare cards eliminates opportunities for fraudsters to obtain SSNs. Similarly, elimination of the SSN from Medicare claims systems and from many DOD systems reduces impact if systems are compromised. Additionally, the time and costs associated with these projects help establish baselines for other government agencies and commercial enterprises as they plan similar projects.

SSN Randomization

The predictability of the Social Security Number Area, Group and Serial number format provided a signal about the validity of a SSN that was useful in determining normal/aberrant behavior and in detecting fraud by banks and anti-fraud services. It allowed these organizations to determine if a presented SSN was likely valid, even if the SSN was not associated with known record in the organization's database. Insight that allowed the organization to determine the "age of the SSN" vs the "age of the person" also helped to detect misrepresentation. Unfortunately, this same signal allowed fraudsters to at least theoretically decode and compromise a person's SSN.

The Carnegie-Mellon team of Acquisti and Gross published a 2009 paper describing how SSNs could be predicted if one knew the location and timeframe of the application. (Acquisti and Gross, 2009, p10975) The requirement to report SSNs on tax filings and the Social Security Administration's 1988 Enumeration at Birth program now added near certainty that for any person born after the mid 80's that the SSN issuance data closely mirrored the person's DOB. The Carnegie Mellon team had already demonstrated that for low volume/low population states, like Delaware, New Hampshire, Vermont and the US Territories with small Area issuance ranges, that it was easy to derive the Area/Group combinations, particularly for the young.

Another Social Security Administration published list, the Death Master File (DMF) provided additional data to train the Carnegie-Mellon algorithm. The DMF contained Name, SSN, Birth Date and Death Date that had been reported to the SSA. Using a portion of this data, the algorithm could be trained to understand the relationship between a specific DOB and not only the Area/Group combination, but the specific spot in the Serial number issuance. Combined with insight on the progression of Group Number assignments, the team could determine a likely cadence of issuance and increase the likelihood that a full SSN could be derived.

In their experiments, Acquisti and Green were able to predict the SSNs on over half a million DMF records for US Born persons with birthdates between January 1973 and December 2003. (Acquisti and Gross, 2013, p10977). The team's success rate reaches 44% for those born after 1988.

Likely because of these concerns about reverse-engineering Social Security Numbers; as well the Social Security Administration policy of assigning full area numbers to states discussed earlier, and the rapid exhaustion of assigned ranges in rapidly growing states, the SSA was running out of number ranges. As seen in Table 2, Florida was working through its third assigned range of Area Numbers and many other sunbelt states had second ranges assigned. Ironically, the High Group listing indicates that less than 50% of the assigned Areas/Group combinations had been used. The 9-digit numbering plan could support nearly a billion SSNs but the assignment rules had created shortages by

locking up numbers in slow growth states. Central issuance of numbers had begun in 1971 (Cronin, 1985) and the requirement to exclusively reserve Areas Number to prevent duplication had passed. In June 2011, the Social Security administration implemented randomization of the issue process. (SSA Randomization webpage, 2018) This had 2 major effects for SSNs issued after the June 25, 2011 date:

1. The Area number no longer had any geographical significance. Area numbers not yet assigned to a specific geography were made available for potential use. (Area 000, 666 and the range 900-999 assigned to the IRS for ITINs are still not used)
2. Group assignments ceased, and the SSA high group list was frozen. Any Area/Group combination not yet issued was available for potential use

SYNTHETIC IDENTITY FRAUD

As an example of the law of unintended consequences, the Social Security Administration likely traded one form of fraud for another when they implemented randomization. The lack of predictability of new Social Security Numbers broke the validation tools that many organizations used to highlight suspect applications. Additionally, because the SSA stopped publishing the High Group List, no intelligence was available to determine whether a given SSN from the previously unissued range had now been issued.

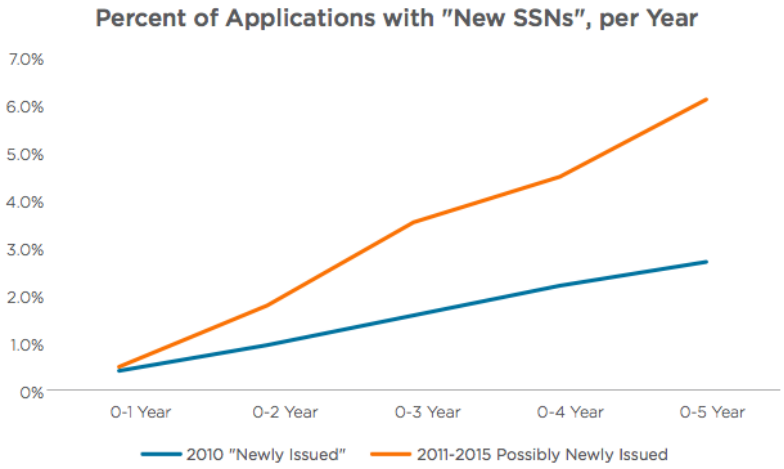
Synthetic fraud, where identities are created from scratch, has been around for years, but was generally a lesser known form of fraud. Financial Institutions and the software and data repositories that served them watched with increasing concerns as applications asserting post-random SSNs flooded in with no ability to verify the authenticity of the asserted Social Security Number.

ID Analytics reported in a 2017 whitepaper that the rate of new, post random SSNs asserted to Financial Institutions, telecom providers and other enterprises had increased significantly in the period following SSN randomization. (IDA Labs, 2017) It is normal to see new Social Security Numbers asserted in commerce as

- Juveniles achieve age 18 and apply for services, and
- Immigrants establish new financial relationships as part of their process of settling into society.

In figure 5 below, ID Analytics depicted the presence of "new" SSNs across a five-year window prior to randomization in blue. This line has a consistent slope and indicates no abnormal behavior. The orange line depicts the presence of "new" SSNs after the 2011 randomization rollout. In addition to the immediate increase in slope, the rate of assertion indicates some variability which is also suggestive of abnormal behavior.

Figure 5- ID Analytics: Comparison of the Natural Growth of New SSNs Pre- and Post-Randomization



In order to determine if there is another explanation for the dramatic increase in fraud, we should look to see if there is a likely population increase in individuals who would newly appear on the file.

Using the 2002 GAO statistics of 5.57M new SSNs per year we can approximate the following ratios:

- 4.23M or 76% of the total SSNs issued in that year, and likely in following years; were issued to citizens. Because of the Enumeration at Birth Program, these citizen SSNs are largely issued to children.
    - A review of census birthrate data indicates that the birth rate has actually declined over the period 1990-2016 from 16.7/1000 to 12.2/1000 (Statista, 2018)
- 1.34M SSNs (or 24%) were issued to immigrants.

- The Migration Policy Institute indicates that in 2016, 1.49 million foreign-born individuals moved to the United States and that the rate of immigration has remained relatively constant since 2000. (MPI, 2018)

Therefore, the shift in behavior observed is not likely justified by benign factors.

This unverifiable population has created significant stress for Financial Institutions and the issue of Synthetic Identities has become a topic of great concern to regulators and institutions. In February 2018, a Bipartisan Group of Senators urged acting Social Security Administration Commissioner Nancy Berryhill to take immediate action to support real-time verification of Name/SSN combinations with SSA database by registered, vetted organizations. (Berryhill letter, 2018)

As of March 25, 2018, the Social Security Administration has not responded.

ALTERNATE IDENTITY SYSTEMS

As seen in the DOD and Medicare use cases, elimination of the Social Security Number from the myriad of use cases across government and the private sector is a complex and costly process.

Substitution with a new numbering scheme has been suggested, as have additional security layers. Changing the rolling order of sequence number issuance to reduce predictability and the inclusion of a separate check-digit field to reduce typos has also been proposed (Winkler, 2009). Randomization, as discussed above, is designed to extend the life of the Social Security Number issuance pool and reduce predictability; which is both good and bad.

Many other countries have National Identity systems and publish the identifiers for people without the same level of identity risk we experience in the US. One example that the US could examine is that of the Icelandic kennitala, translated as name-number or identity number (Watson 2010) This ten-digit number is assigned at a young age, much like the US Social Security Number and contains the 6-digit DOB, (DDMMYY) a 2-digit random number, a check-digit and a digit representing the century of birth. It functions as an alternative to a name, and public databases are available for lookup/conversion of a person's kennitala. (Watson, 2010, p56).

The kennitala functions in many of the ways that the SSN gained use in the US and for the same reasons. It provides a common linking key across databases and assists in data sharing. Given Iceland's patronymic naming system, it creates a critical method to distinguish one John Smith (or Jòn Jòhanson) from another.

One key difference between the SSN and the kennitala is that the Icelandic kennitala is used solely to refer to a person, not to authenticate them. The number is known to be public, not presumed secret such as the SSN is in the US, and therefore an authentication layer, which varies by use case and transaction risk level is used in conjunction with any assertion of the kennitala. Iceland has a national identity card, but it is not regularly used (Watson, 2010, p66). Instead, the kennitala is placed on driver's licenses and on credit cards, both of which commonly have pictures embedded in the document. The presentation of credible physical proof of 'ownership' of the kennitala reduces fraud. In some use cases, such as interactions with social services agencies, presentation of physical proof is mandatory (Watson, 2010, p64). Because the kennitala is used as a reference and other levels of verification/authentication supplement it, Watson indicates the level of identity theft is low

The kennitala is not universally popular- Icelandic civil liberty advocates have similar criticisms as their US counterparts have regarding the Social Security number. A particular concern of civil libertarians is that linkages across state agencies and

commercial entities creates conditions where mass digital surveillance can be accomplished with minimal effort. (Watson, 2010, p74)

Similar national registration schemes are illustrated by Sweden's personnummer (Gronlund, 2010) and Norway's fødselsnummeret or 'birth-number' (Frestad, 2017). These systems exhibit many of the same attributes: universal registration, public disclosure of the number, additional authentication and verification requirements and low level of ID theft.

CONCLUSIONS

The SSN is integral to modern American life. Without a conscious, directed plan it has become the default identifier in our relationships with government agencies, financial institutions, our employers and many other commercial interactions. The SSN was created for a singular purpose; to track the wage contributions of U.S. citizens to support social welfare programs. The expansion of the use of the SSN over time has opened a Pandora's box of unintended consequences.

Why does the United States appear to have this unique and significant level of identity risk? There are a number of reasons. As a nation, we are in denial that we have (or need) a National Identifier; all-the-while using the Social Security Number as our de-facto National ID. Because of the unofficial nature of the SSN as this national identifier, we have failed to create adequate levels of security, policy and process around its use. The number format itself provides no security and introduces risk, with no easy way to determine either the validity of a given number or authoritative association of a SSN with a specific person. Because we lack policy around its use, the number has proliferated to many use cases and most importantly, has been incorrectly assumed to be a method of authenticating an identity instead of an identifier or confirming element for matching purposes.

The use of the SSN as an authenticator rather than an identifier is the critical factor in the identity theft risks created by over-disclosure, data breaches and other forms of compromise. We have created an environment where the SSN 'unlocks' the identity. Names, addresses and phone numbers are freely published in phone books, church directories and other rosters with little concern by citizens. The SSN, on the other hand has power; but that power exists only because we grant it special status and use it for the wrong purpose.

We could replace the SSN with another number, but until we stop using the SSN as authentication, we will continue to struggle with stolen and fraudulently asserted identities based on the SSN or whatever we replace it with. Notwithstanding the debate on whether the US <u>needs</u> a common national identifier, any replacement needs to incorporate three major attributes:

1. Break the linkage between an Identifier and an Authenticator
    - A combination of in-person proofing, pictures, biometrics, PKI or other tools can be layered into the revised identity system
2. Publish the register of Names and Numbers, to eliminate the Identifier/Authenticator link and to enhance accuracy of the identifier and eliminate synthetic identities
3. Consider addition of a check-digit, to reduce keying error and enhance security

Rather than an expensive and difficult wholesale replacement, we could accomplish the same outcome and retain all the value of common reference and accurate linking by changing our approach to how we use and share the SSN.

APPENDICES

Financial Services Roundtable:
Federal Laws and Regulations Related to Financial Institutions' Obtaining Social Security Numbers

Statute & Regulation	Social Security Number Requirement	Retention/Disposal Provisions
A. BSA/AML		
Customer Identification Program ***31 C.F.R. § 1020.220***	**Prior to opening an account**, the bank/thrift/credit union must, at a minimum, obtain the customer's name, date of birth, address (residential or business), and an **identification number** (can be taxpayer identification number).	The bank must retain identifying information for **five years after the account is closed**.
Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks *(31 C.F.R. § 1010.415)*	**No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 or more in currency unless it maintains records of the following information,** which must be obtained for each issuance or sale of one or more of these instruments to any individual purchaser which involves currency in amounts of $3,000-$10,000 inclusive: **If the purchaser does not have a deposit account with the financial institution:** (A) The name and address of the purchaser; (B) The **social security number** of the purchaser, or if the purchaser is an alien and does not have a social security number, the alien identification number; (C) The date of birth of the purchaser; (D) The date of purchase; (E) The type(s) of instrument(s) purchased; (F) The serial number(s) of the instrument(s) purchased; and (G) The amount in dollars of each of the instrument(s) purchased.	Records required to be kept shall be retained by the financial institution for a period of **five years** and shall be made available to the Secretary upon request at any time.
Beneficial Ownership *31 C.F.R. § 1010.230 (effective May 11, 2018**)***	Financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers. As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and **social security number** or other government	A financial institution must retain the records for five years after the date the account is closed.

	identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.	
B. Consumer Financial Products and Services		
Application for a residential mortgage loan (Truth in Lending Act) *12 C.F.R. §§ 1026.3(a)(3)(ii); 1026.25*	For residential mortgage transactions, an application consists of the submission of the consumer's name, the consumer's income, the consumer's **social security number** to obtain a credit report, the property address, an estimate of the value of the property, and the mortgage loan amount sought.	A creditor shall retain evidence of compliance for **two years** after the date disclosures are required to be made or action is required to be taken.
Electronic Fund Transfer Act – Error Notice *12 C.F.R. §§ 1005.11 and 1005.13*	A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that: (i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, on which the alleged error is first reflected; (ii) Enables the institution to identify the consumer's name and account number; and(iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section. ***Content of error notice.*** The notice of error is effective even if it does not contain the consumer's account number, so long as the financial institution is able to identify the account in question. For example, the consumer could provide a Social Security number or other unique means of identification.	Any person subject to the Act and this part shall retain evidence of compliance with the requirements imposed by the Act and this part for a period of not less than **two years** from the date disclosures are required to be made or action is required to be taken.
C. Privacy/Information Security		
Privacy of Financial Information *12 C.F.R. pt. 332*	**Nonpublic personally identifiable information includes any information a** consumer provides to you to obtain a financial product or service from you.	No specific recordkeeping requirement.

	The regulation: Requires a financial institution to provide notice to customers about its privacy policies and practices; Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.	
Interagency Guidelines Establishing Information Security Standards *12 C.F.R. pt. 364, App. B (and corresponding regs)*	An institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to **sensitive customer information, which includes SSN,** because this type of information is most likely to be misused, as in the commission of identity theft. **Notice to Regulator:** The institution's response program must include procedures for notifying its primary federal regulatory as soon as possible when the institution becomes aware of an incident involving unauthorized access to or uses of **sensitive customer information.** **Notice to Consumer:** When a financial institution becomes aware of an incident of unauthorized access to **sensitive customer information**, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay.	An institution's information security program must ensure the proper disposal of customer information and consumer information.

	However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.	
D. Identity Theft/Consumer Reports		
Red Flags Rule *12 C.F.R. pt. 334, App. J (and corresponding regs)*	Requires financial institutions and creditors to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts: Suspicious personal identifying information includes: • Social security number has not been issued or is listed on the Social Security Administration's Death Master File • Lack of correlation between the SSN range and date of birth • The SSN provided is the same as that submitted by other persons opening an account or other customers.	
Duties of Consumer Reporting Agencies Regarding Identity Theft *12 C.F.R. § 1022.123*	**Consumer reporting agencies shall develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity** where the consumer asserts a good-faith belief that have been a victim of identity fraud or a related crime. **Examples of information** that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only: *Consumer file match.* The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of **Social Security number**, and/or date of birth.	

Disclosure by CRA of Consumer File to Consumer; Free Annual Report; *15 U.S.C. §§ 1681g, 1681h, 1681j(a); 12 C.F.R. pt. 1022, subpart N.*	Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer **all information in the consumer's file** at the time of the request, except that if the consumer to whom the file relates requests that the first five digits of the SSN not be included, and the reporting agency has adequate proof of the identity of the requester, the reporting agency shall so truncate the disclosure. A CRA shall require, as a condition of making that disclosure, that the consumer furnish **proper identification**. Free Annual Reports: There is a centralized source for requesting annual file disclosures from nationwide CRAs which collects only as much **personally identifiable information** as is reasonably necessary to properly identify the consumer and to process the transaction requested by the consumer. Any **personally identifiable information** collected from consumers as a result of a request for annual file disclosure, or other disclosure required by the FCRA, made through the centralized source, may be used or disclosed by the centralized source or a nationwide consumer reporting agency only: (1) To provide the annual file disclosure or other disclosure required under the FCRA requested by the consumer; (2) To process a transaction requested by the consumer at the same time as a request for annual file disclosure or other disclosure; (3) To comply with applicable legal requirements, including those imposed by the FCRA and this part; and (4) To update personally identifiable information already maintained by the nationwide consumer reporting agency for the purpose of providing consumer reports, provided that the nationwide consumer reporting agency uses and discloses the updated personally identifiable information subject	

	to the same restrictions that would apply, under any applicable provision of law or regulation, to the information updated or replaced.	

(Financial Services Roundtable, 2018)

REFERENCES

Ablon, L., Heaton, P., Levery, D., & Romaosky, S. (2016). *Consumer Attitudes Toward Data Breach Notifications*. Boston, MA: Rand Corporation.

Acquisti, A., Gross, R., & Fienberg, S. (2009). Predicting Social Security Numbers from Public Data. *Proceedings of the National Academy of Sciences of the United States of America*, *106*(27), 10975-10980.

The Alias Among Us: The Homeland Security and Terrorism Threat From Document Fraud, Identity Theft, and Social Security Number Misuse: Hearings before the Committee on Finance, 108th Cong., 1st Session (2003).

Altmeyer, A. J. (1970). *The Formative Years of Social Security*. University of Wisconsin.

Anthony, R. N., & Sears, M. V. (1963). Who's That? *Harvard Business Review*, 65-71.

Bank Secrecy Act of 1970, 31 U.S.C. §§ 103-34 (1970).

Berk, S. (2014, January 30). Kennitala, Explained. Retrieved March 25, 2018, from Iceland Review website: http://icelandreview.com/stuff/views/2006/03/29/kennitala-explained

Birth Rate in the United States from 1990 to 2016. Retrieved March 26, 2018, from Statista, The Statistics Portal website: https://www.statista.com/statistics/195943/birth-rate-in-the-united-states-since-1990/

Bisson, D. (2017, September 14). 4 Credit Bureau Data Breaches that Predate the 2017 Equifax Hack. *TripWire*.

Blumenthal, R. (1972, June 19). Police Urge Social Security Numbers on Valuables. *New York Times*.

Cabaseg, C., Ziogas, A., Shehata, M., & Anton-Culver, H. (2016). A Validation Method to Determine Missing Years of Birth in a Cohort Study of Shipyard Workers Using Social Security Number. *Journal of Occupational & Environmental Medicine, 58*(6), 631-635.

Cassidy (Senator- LA), B., McCaskill (Senator- MO), C., Peters (Senator- MI), G., & Scott (Senator- SC), T. (2018, February 12). [Letter to Nancy Berryhill (SSA)].

Congressional Budget Office, Cost Estimate HR 1078 Social Security Number Protection Act of 2006, H.R. Doc., (2006).

Congressional Budget Office, Cost Estimate: HR 5320 Social Security Must Avert Identity Loss (MAIL) Act of 2016, Rep., (2016).

Crandall-Hollick, M., & Lunder, E. (2016, March). *Individual Taxpayer Identification Number (ITIN) Filers and the Child Tax Credit* (Report No. R4420). Washington, DC: Congressional Research Service.

Cronin, M. (1985, June). *Fifty Years of Operations in the Social Security Administration*. Retrieved from https://www.ssa.gov/history/cronin.html

https://www.ssa.gov/history/cronin.html

Crowley, N. (2015). Naked Dishonesty: Misuse of a Social Security Number for an Otherwise Legal Purpose May Not Be a Crime Involving Moral Turpitude After All. *San Diego International Law Journal, 205*, 205-250.

Department of the Army Pamphlet 600–8–14 Personnel-General Army Identification Tags. (2015, November 30). Retrieved August 30, 2017, from Department of the Army- ePubs website: http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/p600_8_14.pdf

DeWitt, L. (2007). The First Controversy over Financing and the Creation of Family Benefits 1935-1939. In *Social Security: A Documentary History* (pp. 94-138). CQ Press.

DeWitt, L. (2010). The Development of Social Security in America. *Social Security Bulletin, 70*(3).

DiSanto, P. (2015). Blurred Lines of Identity Crimes: Intersection of the First Amendment and Federal Identity Fraud. *Columbia Law Review, 115*(4), 941-982.

Exec. Order No. 9397, 8, No 237 Fed. Reg. 16095 (Nov. 30, 1943). Retrieved from https://www.loc.gov/item/fr008237/

Fact Sheet: The Work of the President's Identity Theft Task Force. (2006). Washington, DC: Department Of Justice.

Federal Trade Commission. (2014, May). *Data Brokers: A Call for Transparency and Accountability*.

Federal Trade Commission. (2003, December). *FTC Report to Congress- Under Section 318 and 319 of the Fair and Accurate Credit Transaction Act of 2003*.

Federal Trade Commission. (2019, October). *Consumer Data Broker ChoicePoint Failed to Protect Consumers' Personal Data, Left Key Electronic Monitoring Tool Turned Off for Four Months*.

Federal Trade Commission. *Identity Theft- A Recovery Plan*. (2016, September). Washington, DC

Federal Trade Commission. *Security in Numbers- SSNs and ID Theft*. (2008, December). Washington, DC:

FFIEC BSA AML Examination Manual (FFIEC, Comp.) (2014). Washington, DC: Federal Financial Institution Examiners Council.

Field Hearing on Social Security Numbers and Child Identity Theft: Hearings before the Subcommittee on Social Security, Committee on Ways and Means, 112th Cong., 1st Sess. 79 (2011).

Fifth in a Series of Subcommittee Hearings on Protecting and Strengthening Social Security: Hearings before the Subcommittee on Social Security- House Ways and Means, 109th Cong. (2005).

Former Social Security Administration Employee and Two Others Indicted for Stealing IDs. (2017). In *DOJ release* (p. 1).

Francis, L., & Francis, J. (2017). Chapter 2- Protecting Personal Information. In *Privacy: What Everyone Needs to Know*. New York, NY: Oxford University Press.

Frestad, H. (2017, June). *The Norwegian National Identification Numbering System: The History of a Design Process*. Norwegian University of Science and Technology, Trondheim, Norway.

Gemalto. (2017). *Breach Level Index 2017*. Gemalto.

General Accounting Office, Social Security- Observations on Improving Distribution of Death Information, H.R. Misc. Doc. No. GAO-02-233T, at 7 (2001).

General Accounting Office, Social Security Administration- Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain, H.R. Rep. No. GAO-03-12, at 40 (2003).

General Accounting Office, Social Security Numbers- Improved SSN Verification and Exchange of States' Drivers Records Would Enhance Identity Verification, Doc. No. GAO-03-920, at 35 (2003).

General Accounting Office, Social Security Numbers- Federal Actions Could Further Decrease Availability in Public Records, Though Other Vulnerabilities Remain, S. Rep. No. GAO-07-752, at 45 (2007).

General Accounting Office, Social Security Numbers are Widely Available in Bulk and Online Records, but Changes to Enhance Security are Occuring, S. Rep. No. GAO-08-1009R, at 41 (2008).

General Accounting Office, Identity Theft- Improved Collaboration Could Increase Success of IRS Initiatives Prevent or Reduce Fraud, Rep., at 39 (2017).

General Accounting Office, Social Security Numbers- OMB Actions Needed to Strengthen Federal Efforts to Limit Identity Theft Risk by Reducing Collection, Use and Display, H.R. Doc. No. GAO-17-553, at 45 (2017).

Glick, R. (2016, August 19). Darknet: Where Your Stolen Identity Goes to Live. *Dark Reading*.

Grant, J. (2017, October 27). Scrapping Social Security numbers won't be enough to protect our identities. *The Hill*. Retrieved from http://thehill.com/opinion/technology/357374-scrapping-social-security-numbers-wont-be-enough-to-protect-our-identities

Greenberg, A. (2017, November 19). What is the Dark Web? *Wired*.

Grönlund, A. (2010). Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society*, 195-211.

Harbitz, M. (2015, September). Getting it Right From the Start: The Foundations of National Identification System. In *Harvard FXB Center's 21st Century National Identification Conference*. Symposium conducted at Harvard University, Cambridge, MA. Retrieved from https://cdn2.sph.harvard.edu/wp-content/uploads/sites/52/2016/02/Getting-it-right-from-the-start_MiaHarbitz.pdf

Hearing on Removing Social Security Numbers From Medicare Cards: Hearings before the Subcommittee on Social Security, 112th Cong., 2d Sess. (2012).

IDA Labs. (2017, August). *The Synthetic Epidemic: Understanding Identity Fraud After SSN Randomization*. San Diego, CA: ID Analytics.

Indiana DFI. Identity Thieves Can Ruin Your Good Name. Retrieved February 6, 2018, from Indiana Department of Financial Institutions website: https://www.in.gov/dfi/2549.htm

Internal Revenue Service. (1959). *Form 1040 (1960)*. Retrieved from https://www.irs.gov/pub/irs-prior/f1040--1960.pdf

Internal Revenue Service. (1960). *Form 1040 Instructions (1961)*. Retrieved from https://www.irs.gov/pub/irs-prior/i1040--1961.pdf

Internal Revenue Service. (1960). *Form 1040 (1961)*. Retrieved from https://www.irs.gov/pub/irs-prior/f1040--1961.pdf

Internal Revenue Service. (1961). *Form 1040 (1962)*. Retrieved from https://www.irs.gov/pub/irs-prior/f1040--1962.pdf

In the Courts- SSN. (2009). *Privacy Journal, August,* 76.

The IRS' Case of Missing Children. (1989, December 11). *Los Angeles Times*.

Kim, J., Shin, H. C., Rosen, Z., Kang, J.-H., Dykema, J., & Muehnig, P. (2015). Trends and Correlates of Consenting to Provide Social Security Numbers: Longitudinal Findings from the General Social Survey (1993–2010). *Field Methods, 27*(4), 348-362.

Liebman, J. (2000). Who Are the Ineligible EITC Recipients? *National Tax Journal, 53*(4), 1165-1186. Retrieved from https://sites.hks.harvard.edu/jeffreyliebman/ntjeitc.pdf

Long, W. (1993). *Social Security Numbers Issued: A 20-Year Review*. Retrieved from https://www.ssa.gov/policy/docs/ssb/v56n1/v56n1p83.pdf

Mc Elroy, W., & Watner, C. (Eds.). (2004). *National identification Systems: Essays in Opposition*. Jefferson, NC: McFarland and Co.

McKinley, C., & Frase, R. (1970). Old Age Benefits. In *Launching Social Security; A Capture-and-Record Account, 1935-1937:* (pp. 342-381). Madison, WI: The University of Wisconsin Press.

Medicare Identity Theft Prevention Act of 2012, H.R. Res. HR 1509 (2012).

Michael, K., & Michael, M. G. (2006). Historical Lessons on ID Technology and the Consequences of an Unchecked Trajectory. *Prometheus*, *24*(4), 365-378.

Murphy, P. (2015, June). Military's Use of Social Security Numbers a Vulnerability for Veterans. *KUOW*.

National Archives. Service Numbers and Social Security Numbers. Retrieved August 30, 2017, from National Archives website: https://www.archives.gov/st-louis/military-personnel/social-security-numbers.html

National Driver Register Act of 1982, Public Law 97-364 (1982).

New Medicare Cards Start Mailing in April 2018. Retrieved March 20, 2018, from CMS.GOV website: https://www.cms.gov/medicare/new-medicare-card/nmc-home.html

The 1970 Bank Secrecy Act and the Right of Privacy. (1973). *William and Mary Law Review*, *14*(4), 929-952.

Opria, G. R., & Maraska, D. G. (2007). *An Analysis of the Use of Social Security Numbers Number as Veteran Identification as it Relates to Identity Theft*. Naval Postgraduate School, Monterey, CA.

Parenti, C. (2003). Chapter 6- Of Ones and Zeroes: Digital Surveillance Emerges. In *Surveillance in America from Slavery to the War on Terror*. New York, NY: Basic Books.

Perez, S. (2015, March 5). Capital One's History: From Credit Cards to a Diversified Bank. *Market Realist.* Retrieved from https://marketrealist.com/2015/03/capital-ones-history-credit-cards-diversified-bank

The President's Identity Theft Task Force Report. (2008, September). Washington, DC.

Protecting The Privacy of The Social Security Number From Identity Theft: Hearings before the Committee on Ways and Means, 110th Cong., 1st Sess. (2007).

Puckett, C. (2009). The Story of the Social Security Number. *Social Security Bulletin, 55*(9), 55-74.

Regulation 106: Employees Tax and the Employers Tax Under the Federal Insurance Contributions Act, C.F.R. (Nov., 1936).

Removal of the Social Security Number (SSN) from DoD ID Cards. (2014, September). Retrieved from http://www.cac.mil/Portals/53/Documents/SSNReductionTrifold_201409.pdf

Report of Distribution of Surnames in the Social Security Number file, (Technical Report No. 42004). Baltimore, MD: Social Security Administration.

Schaum, K. (2017). Prepare Your Systems for the Social Security Number Removal Initiative. *Advances in Skin & Wound Care, 30*(8), 350-352.

Scott, J. (2017). *Equifax: America's In-Credible Insecurity*. Washington, DC: Institute for Critical Infrastructure Technology (ICIT).

Scott, J. (2017, January). *Dragnet Surveillance Nation- How Data Brokers Sold Out America*. Washington, DC: Institute for Critical Infrastructure Technology.

Shannon, J. (2009). Applying for a New Social Security Number. *Health Reference Series. Domestic Violence Sourcebook 3rd edition*, *502*(509).

Smith, R. E. *Social Security Numbers: Uses and Abuses*. Providence, RI: Privacy Journal.

Smith, R. E. (2003). The Social Security Number in America: 1935-2000. In C. Watner & W. McElroy (Eds.), *National Identification Systems: Essays in opposition* (pp. 203-223). McFarland.

Social Security Administration. *Social Security: Lawfully Admitted Aliens- When You Need a Number and When You Don't.* (2000).

Social Security Administration *New Numbers for Domestic Violence Victims and others*. (1999). Washington, DC: Social Security Administration.

Social Security Administration. Social Security Number Randomization. Retrieved March 26, 2018, from https://www.ssa.gov/employer/randomization.html

Social Security Administration. *Social Security Numbers for Children* [Pamphlet]. (2000). Washington, DC: Social Security Administration.

Social Security Administration. *Social Security Numbers for Newborns* [Pamphlet]. (1999). Washington, DC: Social Security Administration.

Social Security Administration. (1936). *SSA Informational Circular no 9: Security in Your Old Age*. Social Security Board.

Social Security Administration. (2011). *SS-5 Form v08-2011*. Social Security Administration.

Social Security Administration. SSA POMS- Program Operations Manual, Retrieved from http://policy.ssa.gov/poms.nsf/lnx/0110205505

Social Security Administration Inspector General. (2008, May). *Removing Social Security Numbers from Medicare Cards* (Issue Brief No. A-08-08-18026). Social Security Administration.

Social Security Number Fraud Prevention Act, H.R. HR 624, 115th Cong., 1st. (2017).

Social Security Number Guide. (1992). Tulsa, OK: National Employment Screening Service.

Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy: Hearings before the Energy and Commerce, 109th Cong., Ist Sess. (2006).

Social Security Programs in the United States (Report No. 13-11758). (1997, July). Washington, DC: Social Security Administration.

Sutherland, A. (1994). Gypsy Identity, Names and Social Security Numbers. *PoLAR, 75*, 75-84.

Swendiman, K., & Lanza, E. (2014, February). *The Social Security Number: Legal Developments Affecting Its Collection, Disclosure and Confidentiality* (Report No. RL30138). Washington, DC: Congressional Research Service.

Synovate. (2007, November). *Federal Trade Commission- 2006 Identity Theft Survey Report*. Washington, DC: Federal Trade Commission.

Tax Reform Act of 1976, Public Law 94-455 (1976).

Tax Reform Act of 1986, Public Law 99-514 (1986)

Trainor, S. (2015, July 22). The Long Twisted Story of Your Credit Report. *Time Magazine*.

Treasury Inspector General for Tax Administration. *The Number of Employment-related Identity Theft Victims Is Significantly Greater Than Identified* (Report No. 2017-40-031). Washington, DC: Department of the Treasury.

Tverdek, E. (2008). What Makes Information Public? *Public Affairs Quarterly, 22*(1), 63-77.

Twight, C. (2001, October 17). *Watching You Systematic Federal Surveillance of Ordinary Americans*. Retrieved from Cato Institute website: https://object.cato.org/sites/cato.org/files/pubs/pdf/bp69.pdf

Two Major Protections for SSNs. (2017). *Privacy Journal*, (October), 1.

2017 Data Breach Litigation Report. (2017). Washington, DC: Bryan Cave, LLP.

Use of Social Security as a National Identifier: Hearings before the Subcommittee on Social Security of the Committee on Ways and Means, 102d Cong., 2d Sess. (1991).

Watson, I. (2010). A short history of national identification numbering in Iceland. *Bifröst Journal of Social Science, 4*, 51-89. Retrieved from http://hdl.handle.net/1946/10902

Watson, I. (2015, September). The Icelandic Kennitala. In *Harvard FXB Center's 21st Century National Identification conference*. Symposium conducted at Harvard University, Cambridge, MA. Retrieved from https://cdn2.sph.harvard.edu/wp-content/uploads/sites/52/2016/02/The-Icelandic-kennitala_IanWatson.pdf

Wheatley, M. (2015, November). Capital One Builds Entire Business on Savvy Use of IT. *CIO*.

Williams, B. C., Demitrack, L. B., & Fries, B. (1992). The Accuracy of the National Death Index When Personal Identifiers Other than Social Security Number Are Used. *American Journal of Public Health*, *82*(8), 1145-1147.

Winkler, W. (2009). Should Social Security Numbers Be Replaced by Modern, More Secure Identifiers? *Proceedings of the National Academy of Science*, *106*(27), 10877-10878.

Wooten, J. (2007, October 11). Thinking Right: Illegals and Fake Social Security Numbers. *Atlanta Journal Constitution*.

Wyatt, B., & Wandell, W. (1970). Chapter IV- Registration of Employers and Employees. In T*he Social Security Act In Operation; A Practical Guide To The Federal and Federal-State Social Security Programs*. Graphic Arts Press.

Zong, J., Batalova, J., & Hallock, J. (2018, February 8). Frequently Requested Statistics on Immigrants and Immigration in the United States. Retrieved March 26, 2018, from Migration Policy Institute website: https://www.migrationpolicy.org/article/frequently-requested-statistics-immigrants-and-immigration-united-states#Numbers